TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 10 août 2001 (10.08.01)	
Demande internationale no PCT/FR00/02715	**Référence du dossier du déposant ou du mandataire** 6681WO
Date du dépôt international (jour/mois/année) 29 septembre 2000 (29.09.00)	**Date de priorité** (jour/mois/année) 01 octobre 1999 (01.10.99)
Déposant GUILLOU, Louis etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

10 avril 2001 (10.04.01)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

P. Blanchet (Fax 338.87.40)

no de téléphone: (41-22) 338.83.38

10/089646

JC10 Rec'd PCT/PTO 29 MAR 2002

Express Mail No. EV049900720US

PATENT APPLICATION OF

LOUIS GUILLOU AND JEAN-JACQUES QUISQUATER

ENTITLED

SET OF PARTICULAR KEYS FOR PROVING AUTHENTICITY OF AN ENTITY OR THE INTEGRITY OF A MESSAGE

Docket No. F40.12-0006

TRAITE DE COOPÉRATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 6681WO	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 02715	Date du dépôt international *(jour/mois/année)* 29/09/2000	(Date de priorité (la plus ancienne) *(jour/mois/année)* 01/10/1999
Déposant FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

[X] le texte est approuvé tel qu'il a été remis par le déposant

[ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

[ ] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 00/02715

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 381 523 A (TOKYO SHIBAURA ELECTRIC CO) 8 août 1990 (1990-08-08) page 2, ligne 25 -page 3, ligne 7 ---	1,3,4
A	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande abrégé colonne 2, ligne 40 -colonne 3, ligne 50 colonne 12, ligne 30 -colonne 13, ligne 55 --- -/--	1,5,11

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
14 décembre 2000	29/12/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Masche, C

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS,IEE STEVENAGE,GB, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, colonne de gauche, ligne 3 - ligne 61	1,11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/02715

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0381523 A	08-08-1990	JP 2204768 A	14-08-1990
		JP 3053367 A	07-03-1991
		US 5046094 A	03-09-1991
		JP 3073990 A	28-03-1991
		JP 3072737 A	27-03-1991
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		DE 3876741 T	24-06-1993
		ES 2037260 T	16-06-1993
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

REC'D 13 MAR 2002
WIPO PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 6681.WO	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR00/02715	Date du dépot international *(jour/mois/année)* 29/09/2000	Date de priorité *(jour/mois/année)* 01/10/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
10/04/2001	11.03.2002
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02715

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-42 version initiale

Revendications, N°:

1-11 version initiale

Dessins, feuilles:

1/3-3/3 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☐ des revendications, n^{os} :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-11
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-11
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-11
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) permettant de produire les facteurs premiers dont le produit constitue un module public nécessaire à la mise en oeuvre d'un protocole destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message associé à cette entité. Elle concerne aussi l'utilisation (revendication 11) du procédé de production des facteurs premiers dans un tel protocole.

Etat de la technique:

D1 = EP-A-0 311 470 décrit un tel protocole selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA ; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : "Voici mon identité ; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le protocole d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques dans le protocole selon D1 entraîne des temps de calculs importants.

Invention:

Le procédé selon la revendication 1 permet la production de facteurs premiers

particuliers, respectant les conditions mentionnées dans la revendication, dont le produit constitue un module public n. Ce module public n est utilisé dans un protocole d'authentification défini dans la revendication 11.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les caractéristiques de détermination des facteurs premiers telles que définies dans la revendication 1. De plus ces facteurs premiers permettent le calcul d'un module public n utilisable dans un protocole d'authentification évitant les inconvénients du protocole selon D1. L'objet de la revendication 1 implique par conséquent une activité inventive (article 33(3) PCT).

La revendication 11 concerne un protocole d'authentification utilisant un module public n constitué par le produit de facteurs premiers déterminés par le procédé selon la revendication 1. Elle remplit donc de ce fait les conditions de l'article 33 PCT.

Les revendications 2 à 10 dépendent de la revendication 1 satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Irrégularités dans la demande internationale

Les expressions entre parenthèses utilisées dans les revendications ne sont pas considérées comme des signes de référence au sens de la règle 6.2 b) PCT mais sont essentielles à la définition de l'invention. Les parenthèses devraient donc être supprimées.

Observations relatives à la demande internationale

La formulation "Dans un procédé..., le procédé selon l'invention comprenant l'étape..." n'indique pas clairement (Article 6 PCT) si il est demandé une protection pour la méthode de calcul des facteurs premiers p_i et/ou des nombres de bases g_i servant dans le procédé d'authentification d'entité/message ou pour ce dernier procédé lui-

même.

Il semble que la revendication 1 aurait du utiliser la formulation suivante:
"Procédé de production de f facteurs premiers p_i et/ou de m nombres de bases g_i, lesdits facteurs premiers et nombres de base étant utilisés dans un procédé destiné à prouver à une entité contrôleur...".

L'expression "paramètres dérivés de ceux-ci" dans la revendication 1 n'est pas claire car non limitative.

Translation

6

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

10/089646

Applicant's or agent's file reference 6681WO	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/02715	International filing date (*day/month/year*) 29 September 2000 (29.09.00)	Priority date (*day/month/year*) 01 October 1999 (01.10.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant FRANCE TELECOM		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

RECEIVED
OCT 0 9 2002
Technology Center 2100

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 April 2001 (10.04.01)	11 March 2002 (11.03.2002)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/02715

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:
pages 1-42, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the claims:
pages 1-11, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the drawings:
pages 1/3-3/3, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

*** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-11	YES
	Claims		NO
Inventive step (IS)	Claims	1-11	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-11	YES
	Claims		NO

2. Citations and explanations

The invention concerns a method (Claim 1) for producing prime factors of which the product constitutes a public module necessary for implementing a protocol for proving to a controller entity the authenticity of an entity and/or the integrity of a message associated with said entity. It also concerns the use (Claim 11) of the method for producing prime factors in such a protocol.

Prior art:

D1 (EP-A-0 311 470) describes such a protocol according to which an entity called "trusted authority" assigns an identity to each entity called "witness" and calculates its RSA signature; during a personalization process, the trusted authority gives an identity and signature to the witness. Subsequently, the witness states: "This is my identity; I know its RSA signature". The witness proves that it knows the RSA signature of its identity without disclosing it. Using the public key for RSA verification distributed by the trusted authority, an entity called "controller" verifies, without reading it, that the RSA signature corresponds to the stated identity. The mechanisms using this protocol operate "without transfer of knowledge": the witness does not know the private RSA

key with which the trusted authority signs a large number of identities.

Problem:

The use of the RSA technology makes the authentication protocol susceptible to so-called "multiplicative" attacks; moreover, the work load related to the arithmetic operations in the protocol according to D1 requires a significant amount of computing time.

Invention:

The method according to Claim 1 enables specific prime factors to be produced, which meet the conditions mentioned in the claim, and the product of which constitutes a public module n. This public module n is used in an authentication protocol defined in Claim 11.

None of the documents cited in the international search report discloses or suggests the features of determining prime factors as defined in Claim 1. Moreover, said prime factors enable a public module n that can be used in an authentication protocol to be calculated, overcoming the disadvantages of the protocol according to D1. The subject matter of Claim 1 therefore involves an inventive step (PCT Article 33(3)).

Claim 11 concerns an authentication protocol using a public module n consisting of the product of prime factors determined by the method according to Claim 1. It therefore meets the requirements of PCT Article 33.

Claims 2 to 10, which are dependent on Claim 1, therefore likewise satisfy, as dependent claims, the PCT

requirements of novelty and inventive step.

Certain defects in the international application

The expressions in parentheses used in the claims are not considered to be reference signs (PCT Rule 6.2(b)), but are essential to the definition of the invention. The parentheses should therefore be removed.

Certain observations on the international application

The wording "In a method ..., the method according to the invention, including the step ..." does not clearly indicate (PCT Article 6) whether protection is being sought for the method of calculating prime factors p_i and/or base numbers g_i for use in the entity/message authentication method, or for the latter method *per se*.

It appears that Claim 1 should have used the following wording: "Method for producing f prime factors p_i and/or m base numbers g_i, said prime factors and base numbers being used in a method for proving to a controller entity ...".

The expression "parameters derived therefrom" in Claim 1 is unclear because it is non-limiting.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

29 DEC. 2000

Expéditeur : L'ADMINISTRATION CHARGEE DE LA RECHERCHE INTERNATIONALE

PCT

NOTIFICATION DE TRANSMISSION DU RAPPORT DE RECHERCHE INTERNATIONALE OU DE LA DECLARATION

(règle 44.1 du PCT)

Destinataire

LE NOBEL
A l'att. de VIDON, P.
2, allee Antoine Becquerel
BP 90333
35703 Rennes Cedex 7
FRANCE

Date d'expédition *(jour/mois/année)*	29/12/2000
Référence du dossier du déposant ou du mandataire: 6681WO	**POUR SUITE A DONNER** voir les paragraphes 1 et 4 ci-après
Demande internationale n°: PCT/FR 00/ 02715	Date du dépôt international *(jour/mois/année)* 29/09/2000
Déposant: FRANCE TELECOM et al.	

1. [X] Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.

Dépôt de modifications et d'une déclaration selon l'article 19 :
Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale ; pour plus de précisions, voir cependant les notes figurant sur la feuille d'accompagnement.

Où? Directement auprès du Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse
n° de télécopieur: (41-22)740.14.35

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.

2. [ ] Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2)a), est transmise ci-joint.

3. [ ] **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

[ ] la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

[ ] la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.

4. **Mesure(s) consécutive(s) :** Il est rappelé au déposant ce qui suit:

Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90*bis*.1 et 90*bis*.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.

Dans un délai de **19 mois** à compter de la date de priorité, le déposant doit présenter la demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit reportée à 30 mois à compter de la date de priorité (ou même au-delà dans certains offices).

Dans un délai de **20 mois** à compter de la date de priorité, le déposant doit accomplir les démarches prescrites pour l'ouverture de la phase nationale auprès de tous les offices désignés qui n'ont pas été élus dans la demande d'examen préliminaire international ou dans une élection ultérieure avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou qui ne pouvaient pas être élus parce qu'ils ne sont pas liés par le chapitre II.

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hans Pettersson

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le Guide du déposant du PCT, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "Instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou a une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains Etats.

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand? Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment? Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/peuvent accompagner les modifications?

Lettre (instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

!SDOCID: <XSISA220NOFRP4_I_>

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

i) la revendication n'est pas modifiée;

ii) la revendication est supprimée;

iii) la revendication est nouvelle;

iv) la revendication remplace une ou plusieurs revendications telles que déposées;

v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 15 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."

2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."

3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15,16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."

4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1-10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendiations 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demandeinternationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)"

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications auprès du Bureau international, déposer également une copie de ces modifications auprès de l'administration chargée de l'examen préliminaire international (voir la règle 62.2a), première phrase).

Conséquence au regard de la traduction de la demande internationalelors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle-ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du Guide du déposant du PCT.

SDOCID: <XSISA220NOFRP4_I_>

TRAITE DE COOPÉRATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
6681WO		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 02715	29/09/2000	01/10/1999
Déposant		
FRANCE TELECOM et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

[X] le texte est approuvé tel qu'il a été remis par le déposant

[ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° _____

[ ] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 00/02715

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 381 523 A (TOKYO SHIBAURA ELECTRIC CO) 8 août 1990 (1990-08-08) page 2, ligne 25 -page 3, ligne 7 ---	1,3,4
A	EP 0 311 470 A (TELEDIFFUSION FSE ;FRANCE ETAT (FR); PHILIPS NV (NL)) 12 avril 1989 (1989-04-12) cité dans la demande abrégé colonne 2, ligne 40 -colonne 3, ligne 50 colonne 12, ligne 30 -colonne 13, ligne 55 --- -/--	1,5,11

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
14 décembre 2000	29/12/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Masche, C

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	QUISQUATER J -J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS,IEE STEVENAGE,GB, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 page 906, colonne de gauche, ligne 3 - ligne 61	1,11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 00/02715

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0381523 A	08-08-1990	JP 2204768 A	14-08-1990
		JP 3053367 A	07-03-1991
		US 5046094 A	03-09-1991
		JP 3073990 A	28-03-1991
		JP 3072737 A	27-03-1991
EP 0311470 A	12-04-1989	FR 2620248 A	10-03-1989
		AT 83573 T	15-01-1993
		AU 2197188 A	23-03-1989
		CA 1295706 A	11-02-1992
		DE 3876741 A	28-01-1993
		DE 3876741 T	24-06-1993
		ES 2037260 T	16-06-1993
		FI 884082 A,B,	08-03-1989
		JP 1133092 A	25-05-1989
		KR 9608209 B	20-06-1996
		US 5218637 A	08-06-1993
		US 5140634 A	18-08-1992

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: L'ADMINISTRATION CHARGEE DE L'EXAMEN PRELIMINAIRE INTERNATIONAL

14 MARS 2002

Destinataire:

VIDON, P.
CABINET PATRICE VIDON
Le Nobel
2, allée Antoine Becquerel
BP 90333
F-35703 RENNES Cedex 7
FRANCE

PCT

NOTIFICATION DE TRANSMISSION DU RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(règle 71.1 du PCT)

Date d'expédition *(jour/mois/année)*	11.03.2002

Référence du dossier du déposant ou du mandataire	**NOTIFICATION IMPORTANTE**
6681.WO	

Demande internationale No.	Date du dépot international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR00/02715	29/09/2000	01/10/1999

Déposant
FRANCE TELECOM et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. **RAPPEL**

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Losrqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international	Fonctionnaire autorisé
Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Barrio Baranano, A Tél.+49 89 2399-8621

Formulaire PCT/IPEA/416 (juillet 1992)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 6681.WO	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR00/02715	Date du dépot international *(jour/mois/année)* 29/09/2000	Date de priorité *(jour/mois/année)* 01/10/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
10/04/2001	11.03.2002
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02715

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-42 version initiale

Revendications, N°:

1-11 version initiale

Dessins, feuilles:

1/3-3/3 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.
   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
   ☐ remis ultérieurement à l'administration, sous forme écrite.
   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

- ☐ de la description, pages :
- ☐ des revendications, n^{os} :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-11
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-11
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-11
	Non :	Revendications	

2. Citations et explications
   voir feuille séparée

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne un procédé (revendication 1) permettant de produire les facteurs premiers dont le produit constitue un module public nécessaire à la mise en oeuvre d'un protocole destiné à prouver à une entité contrôleur l'authenticité d'une entité et/ou l'intégrité d'un message associé à cette entité. Elle concerne aussi l'utilisation (revendication 11) du procédé de production des facteurs premiers dans un tel protocole.

Etat de la technique:

D1 = EP-A-0 311 470 décrit un tel protocole selon lequel une entité appelée "autorité de confiance" attribue une identité à chaque entité appelée "témoin" et en calcule la signature RSA ; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : "Voici mon identité ; j'en connais la signature RSA.". Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée "contrôleur" vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant ce protocole se déroulent "sans transfert de connaissance": le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités.

Problème:

L'utilisation de la technologie RSA rend le protocole d'authentification sensible aux attaques dites "multiplicatives"; d'autre part la charge de travail liée aux opérations arithmétiques dans le protocole selon D1 entraîne des temps de calculs importants.

Invention:

Le procédé selon la revendication 1 permet la production de facteurs premiers

particuliers, respectant les conditions mentionnées dans la revendication, dont le produit constitue un module public n. Ce module public n est utilisé dans un protocole d'authentification défini dans la revendication 11.

Aucun des documents cités dans le rapport de recherche international ne divulgue ou suggère les caractéristiques de détermination des facteurs premiers telles que définies dans la revendication 1. De plus ces facteurs premiers permettent le calcul d'un module public n utilisable dans un protocole d'authentification évitant les inconvénients du protocole selon D1. L'objet de la revendication 1 implique par conséquent une activité inventive (article 33(3) PCT).

La revendication 11 concerne un protocole d'authentification utilisant un module public n constitué par le produit de facteurs premiers déterminés par le procédé selon la revendication 1. Elle remplit donc de ce fait les conditions de l'article 33 PCT.

Les revendications 2 à 10 dépendent de la revendication 1 satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Irrégularités dans la demande internationale

Les expressions entre parenthèses utilisées dans les revendications ne sont pas considérées comme des signes de référence au sens de la règle 6.2 b) PCT mais sont essentielles à la définition de l'invention. Les parenthèses devraient donc être supprimées.

Observations relatives à la demande internationale

La formulation "Dans un procédé..., le procédé selon l'invention comprenant l'étape..." n'indique pas clairement (Article 6 PCT) si il est demandé une protection pour la méthode de calcul des facteurs premiers p_i et/ou des nombres de bases g_i servant dans le procédé d'authentification d'entité/message ou pour ce dernier procédé lui-

même.

Il semble que la revendication 1 aurait du utiliser la formulation suivante:
"Procédé de production de f facteurs premiers p_i et/ou de m nombres de bases g_i, lesdits facteurs premiers et nombres de base étant utilisés dans un procédé destiné à prouver à une entité contrôleur...".

L'expression "paramètres dérivés de ceux-ci" dans la revendication 1 n'est pas claire car non limitative.